1906055

NATIONAL INSTITUTE OF TECHNOLOGY PATNA
Department of Computer Science & Engineering
MID SEMESTER EXAMINATION, January - July 2022

B. Tech: Semester-VI

Course Name: Information Security
Maximum Time: 3 hours **Code: CS6404**
Max. Marks: 60

Instruction:

1. Attempt All questions (Question 5 to 8 does not have any alternative).
2. Assume any suitable data, if necessary.
3. The Marks, CO (Course Outcome) and BL (Bloom's Level) related to questions are mentioned on the right-hand side margin.

		Marks	CO	BL
1.a.	What are "Substitution" and "Transposition" techniques? What kind of cipher is the Caesar cipher? Calculate the encryption and decryption for the following plain text P="COME TO MY HOME" by using Caesar Cipher with Key k=3?	3+2 +5	CO1, CO3	A
	OR			
2.a.	In an RSA system the public key of a given user is e = 31, n =3599. What is the private key of the user?	2	CO3	R, U
b.	In a public key system using RSA, the cipher text intercepted is C=10 which is sent to the user whose public key is e=5, n=35. What is the plaintext M?	8		
3.	Explain Feistel Cipher structure of Data Encryption Standard also describe the strength of DES algorithm.	10	CO2	E, C
	OR			
4.	Explain Sub key generation Process in Simplified DES algorithm with key 10011010 01000000 11010101 11111000 01001000 11111010 10011001 01000011	10	CO2	E, C
5.	What is the purpose of S-box in DES? Select the substitution value from the sbox for a block value 33 (in decimal).	4+6	CO4	P
6.	List the security services provided by digital signature. Write and explain the Digital Signature Algorithm with a diagram.	3+7	CO3	U
7.	Explain the initial permutation process of the RC4 algorithm. Describe the RC4 Key-scheduling algorithm (KSA) with a net diagram.	3+7	CO2	R
8.	Differentiate among verification and authentication. What are the different ways of authentications? Explain about them. How can access control be enforced?	2+2+ 4+2	CO1	E

s-box	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Table 1. s-box for question no. 5

****End of Questions****

Level	Bloom's Taxonomy
1	Remembering (R)
2	Understanding (U)
3	Applying (P)
4	Analyzing (A)
5	Evaluate (E)
6	Create (C)

Course Outcomes:

At the end of the course, a student should have:

CO	Outcome
1.	Identify the appropriate technologies necessary to solve concrete problems related to confidentiality (cryptographic solutions), integrity (authentication such as biometric), availability (for example, intrusion detection solutions), and privacy protection.
2.	Develop policies and procedures to manage enterprise security risks.
3.	Evaluate and communicate the human role in security systems with an emphasis on ethics, vulnerabilities and training.
4.	Apply cryptography and some key encryption techniques for providing secure solutions
5.	Determine appropriate mechanisms for protecting information systems ranging from operating systems to database management systems and to applications.